Power of One Bit of Quantum Information in Quantum Metrology

Hugo Cable,[1] Mile Gu,[2,3] and Kavan Modi[4]

[1] *Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK*
[2] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*
[3] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117543 Singapore*
[4] *School of Physics, Monash University, Victoria 3800, Australia*

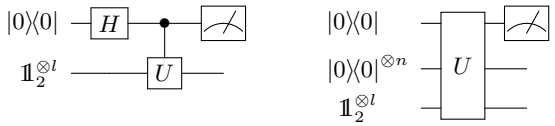
(Dated: April 13, 2015)

We construct a model of quantum metrology inspired by the computational model known as deterministic quantum computation with one quantum bit (DQC1). Using only one pure qubit together with l fully-mixed qubits we obtain measurement precision at the standard quantum limit, which is typically obtained using the same number of uncorrelated qubits in fully-pure states. The standard quantum limit can be exceeded using an additional qubit, which adds only a small amount of purity. We show that the discord in the final state vanishes only in the limit of attaining infinite precision for the parameter being estimated.

Quantum information science has transformed how we view many computation, communication, and precision-measurement tasks. Emerging quantum technologies promise to solve problems that are intractable or impossible using classical counterparts. However, in many cases the origins of quantum enhancements remain the subject of debate. Entanglement unambiguously plays a critical role in many tasks that use pure states, but this often ceases to be true when noise is added to the picture [1]. One of the most studied tasks that uses noisy qubits is provided by a model called DQC1, introduced by Knill and Laflamme [2]. DQC1 performs a specific type of classically-hard computation using highly-mixed quantum states, and thereby seriously challenges the notion that pure-state entanglement plays an essential role in quantum computation.

The task performed by DQC1 is to estimate the normalised trace of a quantum circuit U that acts on a collection of l register qubits, as depicted in Fig. 1(a). The initial state comprises one "clean" pure qubit together with register qubits that are maximally mixed, and only unitary gates are used for the computation. Remarkably, the precision of the estimate does not scale with the size of U. It is intuitively clear that DQC1 achieves an exponential speedup over any classical algorithm which finds and sums the 2^l eigenvalues for U, and there is now considerable evidence which supports the existence of a true quantum speedup for DQC1 [3]. Several works have also analysed how the computational power of DQC1 changes as resources, such as additional pure qubits and measurements, are added [4–6], see Fig. 1(b).

Some studies have also investigated the role of entanglement and quantum discord [7, 8] in the speedup achieved by DQC1 [9, 10]. It has been found that the discord generated at the output of DQC1 [11], by unitary transformations which are randomly selected according to the Haar measure, remains a fixed proportion of the maximum possible as the unitary transformations increase in size. However, the amount of entanglement generated by these unitary transformations is vanishing. It is not yet known that happens to entanglement or discord



(a) DQC1-complete

(b) n-clean qubit model

FIG. 1. *Circuits for DQC1.* (a) A DQC1-complete problem is to compute the normalised trace of a unitary transformation. For the circuit, a Hadamard gate is applied to the control qubit followed by controlled-unitary transformation on the register, and measurement of the control. After several runs of the circuit, an estimate is obtained for $\langle\sigma_x\rangle + i\langle\sigma_y\rangle = \mathrm{tr}(U)/2^l$. The precision of this estimate depends only on the number of runs of circuit. The protocol also works when the control qubit is partially pure at the start – as given by the state given in Eq. (5). In this case, the number of runs must be increased by a factor $1/\epsilon^2$ to achieve the same precision as when the control qubit is initially pure. (b) In the general DQC1 problem, an additional $n \sim \log(l)$ pure qubits can be introduced without altering the computational power of this model [4, 5].

at intermediate steps in a DQC1 computation. In contrast, it well known for pure-state quantum computation that unbounded entanglement is necessary for exponential speedups when using circuits composed of gates of bounded size [1].

We now turn to quantum metrology, and the problem of achieving quantum advantage for precision in the task of phase estimation, which is used for highly-sensitive measurements of physical parameters [12–14]. Phase-estimation strategies that cannot exploit quantum features are subject to the *standard quantum limit* (SQL) for precision, given by $\Delta\phi = 1/\sqrt{n}$ where n particles are used as probe and ϕ is the parameter to be estimated. For example, this limit applies when n single pure qubits in the $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ state are used to measure the phase for a Pauli rotation

$$u_\phi = e^{i\phi\mathfrak{g}} \quad \text{where} \quad \mathfrak{g} = |1\rangle\langle 1|\,. \tag{1}$$

However, when a GHZ state $|+_n\rangle = (|0\rangle^{\otimes n} + |1\rangle^{\otimes n})/\sqrt{2}$ is used as the probe state with $G = \sum_{j=1}^{n} \mathfrak{g}_j$, the precision scales at the Heisenberg limit $\Delta\phi = 1/n$, which is the best precision achievable [13].

Inspired by DQC1, we ask whether a large ensemble of mixed qubits can be used as the basis of a powerful sensor. We consider a model where only one (or few) clean qubits are accessible, and only one qubit can be measured at the end [15]. Physical systems where our model is most relevant include NMR [16–18] and some cold-atom systems [19, 20]. For these systems often only bulk operations on the register qubits are available — which is so say the same operation is applied to every register qubit, optionally under global control. Hence, we add a bulk-operations constraint to our model.

For mixed-state models of phase estimation, recent results challenge any presupposed link between entanglement and quantum advantage for measurement precision. Ref. [21] considers an algorithm for multi-parameter estimation using DQC1. This algorithm uses an adaptive protocol based on a series of estimates with different interactions times, to achieve a final precision scaling with the inverse total interaction time. Ref. [22] analyses the situation where a unitary circuit is used to prepare probe states from n uncorrelated qubits in the state ρ_ϵ given below in Eq. (5). Strategies using probe states with only classical correlations [23], which is to say they are diagonal in the σ_z basis up to local-unitary transformations [24], are compared with strategies with exploit entanglement and quantum discord (defined as in [25]). It was found that circuits which generate non-classical correlations can achieve a quadratic quantum advantage compared to circuits generating only classical correlations at fixed ϵ in Eq. (5). This result holds even for small values of ϵ where there is no entanglement but large amounts of discord, and the amount of discord also grows with n. Another recent analysis considers phase estimation using an interferometer, where the spectrum of the interferometer Hamiltonian is fixed but not its eigenbasis. The authors found that the minimum amount of statistical information that can be extracted about the unknown phase in the problem also constitutes a measure of the discord-type correlations in the probe state [26].

Parameter estimation.— In the classical theory for parameter estimation [27] a probability distribution $\mathbf{p}$ is subjected to a process that is a function of a single parameter ϕ. The process alters the initial distribution $\mathbf{p}$ into $\mathbf{p}(\phi)$, which depends on the value of ϕ. Differentiating between the initial and the final distributions allows for the determination of the value of ϕ. The uncertainty in this value is bounded by the Fisher information, which is given by:

$$\Delta\phi \geq \frac{1}{\sqrt{F}}, \quad \text{with} \quad F = \sum_k \frac{[\partial_\phi p_k(\phi)]^2}{p_k(\phi)} \tag{2}$$

and p_k is the probability for observing outcome k. The above inequality is the Cramér-Rao bound [28, 29].

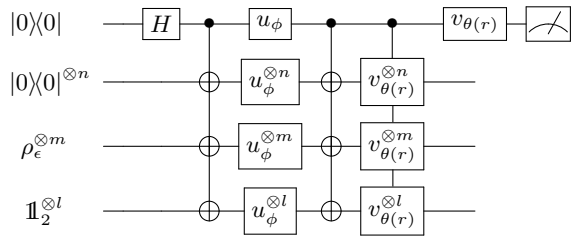


FIG. 2. Illustration of our general scheme for phase estimation: There are n pure qubits, m semi-pure qubits, and l fully-mixed qubits ($\mathbb{1}_2 = \mathbb{1}/2$). The first qubit is the control, and the remaining qubits constitute the register. Only bulk operations are permitted for gates used to prepare the probe state and implement the readout procedure. A bulk CNOT is used to prepare the probe, and then each qubit is subjected to the unitary operation given in Eq. (1) for which ϕ is to be determined. The readout procedure is adaptive: $\theta(r)$ is the estimate for ϕ after the first $r-1$ rounds. This value is used to configure the readout circuit, which is a CNOT followed by controlled-$v_{\theta(r)}$ on all qubits of the register, and measurement on the control.

When using a quantum system, the initial and final probability distributions are replaced by density operators σ and $\sigma(\phi)$ respectively. The final state is measured by a positive operator valued measure (POVM) $\{\Pi_k\}$ to yield classical probabilities $p_k = \mathrm{tr}[\Pi_k \sigma(\phi)]$, from which F in Eq. (2) can be computed. If the process which is parameterized by ϕ is unitary, then the Fisher information when optimised over all POVMs is given by the quantum Fisher information [30]:

$$F_\mathrm{q} = 4 \sum_{i>j} \frac{(\lambda_i - \lambda_j)^2}{\lambda_i + \lambda_j} \left| \langle \psi_i | G | \psi_j \rangle \right|^2, \tag{3}$$

where $\{\lambda_i\}$ are the eigenvalues,$\{|\psi_i\rangle\}$ are the eigenvectors of σ, and G is the Hamiltonian generator of the phase shift. This formula for F_q is very powerful: It yields the lower bound for the precision of ϕ without needing the explicit form of the optimising POVM, and enables a straightforward comparison between different initial states.

The setup.— Our model uses three registers: one with n pure qubits; one with m qubits with finite purity as given in Eq. (5); and one with l fully-mixed qubits. Along with these three registers, there is one pure qubit in state $|0\rangle$ which serves as the control. The total initial state is

$$\sigma_0 = |0\rangle\langle 0| \otimes |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \frac{\mathbb{1}^{\otimes l}}{2^l}. \tag{4}$$

with

$$\rho_\epsilon = \frac{1}{2} \begin{pmatrix} 1+\epsilon & 0 \\ 0 & 1-\epsilon \end{pmatrix}, \quad 0 < \epsilon < 1. \tag{5}$$

(Later we will take the limit of $n, m \to 0$ to develop compare our results with DQC1.) To prepare the probe state

σ we apply the Hadamard gate to the control qubit followed by a CNOT gate for all qubits in the register. Next each qubit in the register is allowed to evolve freely under the unitary operation given in Eq. (1). The readout procedure consists of another controlled operation and measurement of the control qubit. The full protocol is shown in Fig. 2.

To compute $F_{\rm q}$ for σ above, we note that σ_0 has eigenvectors of the form $|\pm; B_0^n; B_j^m; B_k^l\rangle$; here B_i^a represents a binary string of length a with 1s appearing i times, and the semicolons separate the control qubit and the three registers. There are $\binom{m}{j}\binom{l}{k}$ such eigenvectors each with eigenvalue

$$\lambda_j^+ = \frac{1}{2^{m+l}}(1+\epsilon)^{m-j}(1-\epsilon)^j \tag{6}$$

when the control qubit is in state $|+\rangle$, and the eigenvalue is $\lambda_j^- = 0$ otherwise. After the first CNOT gate the eigenvectors are

$$\left|\psi_{jk}^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|0; B_0^n; B_j^m; B_k^l\rangle \pm |1; C_0^n; C_j^m; C_k^l\rangle\right), \tag{7}$$

where C_j^a is the NOT of B_j^a, i.e., $|C_j^a\rangle = \sigma_x^{\otimes a}|B_j^a\rangle$.

The generator of the phase shift is $G = \sum_x |1\rangle\langle 1|_x \otimes \mathbb{1}_{\bar{x}}$, where $\mathbb{1}_{\bar{x}}$ is the identity operator on all but xth qubit, and x runs from 1 to $n+m+l$. Next, we note that the components of the eigenstate of the prepared state are eigenvectors G:

$$G|0; B_0^n; B_j^m; B_k^l\rangle = (j+k)|0; B_0^n; B_j^m; B_k^l\rangle, \tag{8}$$

$$G|1; C_0^n; C_j^m; C_k^l\rangle = (n+1+m-j+l-k) \times |1; C_0^n; C_j^m; C_k^l\rangle \tag{9}$$

and therefore

$$\begin{aligned}\langle\psi_{j'k'}^{\pm}|G|\psi_{jk}^{+}\rangle =& \frac{1}{2}(j+k)\langle B_{j'}^{'m}|B_j^m\rangle\langle B_{k'}^{'l}|B_k^l\rangle \\ &\pm \frac{1}{2}(n+m+l-j-k+1) \\ &\times \langle C_{j'}^{'m}|C_j^m\rangle\langle C_{k'}^{'l}|C_k^l\rangle.\end{aligned} \tag{10}$$

Eq. (10) is non-zero only when $j=j'$ and $k=k'$. We note that the numerator of the first term in Eq. (3) is the difference in two eigenvalues, and therefore it is only necessary to consider $\langle\psi_{j,k}^-|G|\psi_{j,k}^+\rangle$. Hence,

$$\begin{aligned}F_{\rm q} &= 4\sum_{j=0}^{m}\binom{m}{j}\lambda_j^+\sum_{k=0}^{l}\binom{l}{k}\left|\langle\psi_{j,k}^-|G|\psi_{j,k}^+\rangle\right|^2 \\ &= l + m(1-\epsilon^2) + (1+n+\epsilon m)^2\,.\end{aligned} \tag{11}$$

We can make several observations concerning Eq. (11): (i) $F_{\rm q}$ is always greater or equal to the SQL value, which is $1+l+m+n$. (ii) The SQL is attained when $m=n=0$, i.e. the case which is analogous to DQC1 [31]. (iii) If ϵ is small (or even 0) there is a linear contribution of m corresponding to size of the register of partially-pure qubits. (iv) $(n+1)^2$ exhibits the well-known quadratic enhancement for entangled pure states of $n+1$ qubits, and there is an additional contribution equivalent to ϵm extra pure qubits.

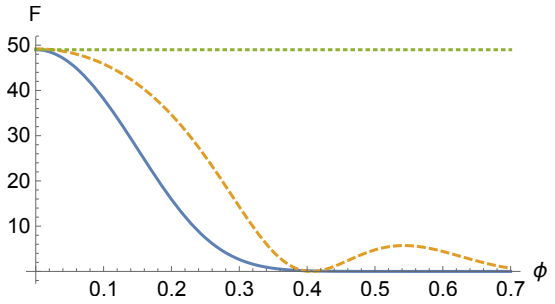


FIG. 3. (Colour online.) Fisher information, F, computed from the probability distribution in Eq. (12) for $n=6$ and $m=l=0$ (dotted); $n=l=0$ and $m=11$ with $\epsilon=0.49$ (dashed); and $l=48$ and $n=m=0$ (solid). F is independent of ϕ when register has no mixed qubits. All three cases have the same value for the quantum Fisher information $F_{\rm q}$.

Readout procedure.— Apart from preparation of the probe state, attention must be given to the bulk-operation requirements for implementing the measurements for the readout procedure. In other words, we need to consider how $F_{\rm q}$ given in Eq. (11) can be attained via a suitable POVM, which in general can require entangled measurements [32]. For our model, the following method suffices (illustrated in Fig. 2): a bulk CNOT gate is performed, followed by a bulk controlled-$v_{\theta(r)}$ where $v_{\theta(r)} = \exp\{-i\theta(r)\sigma_z\}$, and a measurement on the control qubit. $\theta(r)$ here is taken to be the estimate of ϕ following the $(r-1)$th round. The initial estimate $\theta(0)$ can assume no prior knowledge of ϕ. In each successive round our estimate for ϕ is improved, i.e., $|\theta(r)-\phi| < |\theta(r-1)-\phi|$, using an adaptive Bayesian update or maximum-likelihood method to maximize sensitivity [33].

The measurement of the control qubit along the σ_x direction yields probability distribution

$$q^{\pm}(r) = \frac{1}{2}\left(1 \pm x(r)\right) \quad \text{where} \tag{12}$$

$$\begin{aligned}x(r) = {\rm Re}\Big\{ & e^{i(n+1)\omega(r)}\cos^l(\omega(r)) \\ & \times \left[\cos(\omega(r)) + i\epsilon\sin(\omega(r))\right]^m\Big\},\end{aligned} \tag{13}$$

and $\omega(r) = \theta(r) - \phi$. The value for F computed from this probability distribution, using Eq. (2), yields a value that approaches the quantum Fisher information in Eq. (11) as $\omega(r) \approx 0$. That means that the adaptive protocol described above will yield the optimal Fisher information as the estimate $\theta(r)$ approaches ϕ. We have plotted three cases in Fig. 3.

One+ϵ clean qubit metrology.— It is clear that the metrology protocol presented in Fig. 2 is a special case of DQC1 computation, provided $n+m \sim \log(l)$. In fact,

we can think of the circuit as an application of a bulk controlled-unitary operation ${}^{c}U_{\omega(r)}$, where the unitary operation is

$$U_{\omega(r)} = \left(u_\phi^\dagger v_{\theta(r)} \sigma_x \, u_\phi \, \sigma_x\right)^{\otimes l+m+n}. \tag{14}$$

Using this feature we will examine the discord hypothesis for DQC1 due to [10].

However, let us first consider the case where $n = 0$, $m = 1$, and $l > 0$. In this case the probe state σ is entangled for any value of $\epsilon > 0$. This can be understood by noting that a non-positive partial transpose for σ of the state results from applying a CNOT gate on the state in Eq. (5), controlled on $|+\rangle$. Another way to see this is by noting that the value for F_{q} here beats the SQL [34]:

$$F_{\mathrm{q}} = l + 2 + 2\epsilon > l + 2. \tag{15}$$

In other words, even with one qubit with finite purity we can attain better precision than what is possible classically. Adding more qubits to the registers for initially partially-mixed and pure qubits, the entanglement (between the control and registers) will increase as well as the value for F_{q}.

One-pure-qubit metrology.— We now let $n = m = 0$, i.e., consider a $l+1$ qubit state with only one pure qubit and l qubits in fully-mixed state. From Eq. (11) we see that F_{q} has the SQL value of $l+1$ qubits, and that the SQL is attained using only one pure qubit and l fully-mixed qubits. This is highly counterintuitive in the classical setting, where completely-mixed states cannot be used to yield additional information from a phase measurement, and the maximum value for F would be 1 (as attained by a single pure qubit). Therefore the enhancement of F_{q} by l is an entirely quantum-mechanical phenomenon.

It is tempting to say that the resource that enables this enhancement in F_{q} is the entanglement or discord in σ. However, a closer look at σ in the limit $\epsilon \to 0$ reveals that it is an equal mixture of products of eigenstates of σ_x (for which $|-\rangle$ occurs even number of times),

$$\sigma = \frac{1}{2^{l+1}} \left(\mathbb{1}^{\otimes l+1} + \sigma_x^{\otimes l+1}\right), \tag{16}$$

and it is therefore fully-classically correlated [24]. Though σ is separable, and therefore preparable via unrestricted LOCC, it cannot be prepared using bulk LOCC operation. Without the CNOT gate used in the state preparation, which is controlled on a quantum superposition, the register of maximally-mixed qubits cannot be exploited.

At this point we can ask whether there is any discord present in the final state of the circuit. In Ref. [35] it was shown that there is no discord in the output state of a DQC1 circuit when the controlled-unitary operation is Hermitian, i.e. $U = U^\dagger$ in Fig. 1 (see also Refs. [36] and for further details). The unitary operator $U_{\omega(r)}$, in Eq. (14), is Hermitian if and only if $\omega(r) = 0$, i.e. when ϕ is known to perfect precision. Therefore it may be observed that the circuit in Fig. 2 contains discord for all runs except when ϕ is fully known. Repeating this analysis for arbitrary values of l, m, $n > 0$ shows that the final state is always separable, but has finite discord except when $\omega(r) = 0$. The only exception is when $l = m = 0$, in which case the final state has no correlations. We may conclude that noisy input states lead to discordant output states in our model, which sheds new light on the constant level of discord at the output of DQC1 found in Ref. [10].

Discussion.— We have constructed a model of quantum metrology, inspired by DQC1, that uses highly-mixed states as its enabling resource. Our most surprising result arises when the register is taken to be fully mixed. In this case, the probe state is classical correlated, and yet it can only be prepared via a coherent quantum interaction due to the bulk operation constraint of our model. Whilst there is no entanglement or discord in the probe state, we have found that the state at the output always has discord, except in the limit of infinite precision for the phase parameter being estimated. Our model then surpasses the performance of a classical setup when only one qubit in the register has a finite amount of purity. In this case the probe state also has entanglement, which is widely understood to be essential for achieving precision beyond the SQL.

Our results provide support for both entanglement and discord as enabling quantum resources in quantum metrology. Perhaps more importantly, our model shows how a large ensemble of highly-mixed quantum systems can be of great utility for quantum sensing. Since our model only requires bulk coherent operations on the ensemble, it has the potential to enable a scalable quantum technology could challenge state-of-the-art classical sensors in the near future. The biggest practical weakness of our model lies in the fact that if even a single qubit is lost between the first and last controlled gates, all sensitivity is lost — a problem which is shared by any measurement device using pure GHZ states or NOON states in the context of interferometry [12].

Acknowledgements. H.C. is grateful for financial support from the University of Bristol. M.G is supported by the John Templeton Foundation 54914, the National Basic Research Program of China Grant 2011CBA00300, 2011CBA00302 and the National Natural Science Foundation of China Grant 11450110058, 61033001, 61361136003.

[1] R. Jozsa and N. Linden, Royal Society of London Proceedings Series A **459**, 2011 (2003), arXiv:quant-ph/0201143.

[2] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).

[3] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).

[4] A. Ambainis, L. J. Schulman, and U. V. Vazirani, Proc. of the 32nd Ann. ACM Sympo. on Theor. of Comput. , 697 (2000).

[5] P. W. Shor and S. P. Jordan, Quantum Inf. Comput. **8**, 681 (2008).

[6] T. Morimae, K. Fujii, and J. F. Fitzsimons, Phys. Rev. Lett. **112**, 130502 (2014).

[7] W. H. Zurek, Ann. Phys. (Leipzig) **9**, 855 (2000).

[8] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).

[9] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).

[10] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).

[11] Discord is asymmetric with respect to the subsystems for which it is defined. Here we refer to the discord for measurements on the control qubit, while the discord for measurements on the register is always zero when the register is fully mixed. The entanglement between these two partitions is zero when the register is fully mixed.

[12] J. P. Dowling, Contemporary Phys. **49**, 125 (2008).

[13] V. Giovannetti, S. Lloyd, and L. Maccone, Nature Photon. **5**, 222 (2011).

[14] J. L. O'Brien, A. Furusawa, and J. Vučković, Nature Photonics **3**, 687 (2009).

[15] Inclusion of additional measurements would allow for the preparation of pure states from mixed qubits, which fundamentally change the power of the model.

[16] J. A. Jones, S. D. Karlen, J. Fitzsimons, A. Ardavan, S. C. Benjamin, G. A. D. Briggs, and J. J. L. Morton, Science **324**, 1166 (2009).

[17] S. Simmons, J. A. Jones, S. D. Karlen, A. Ardavan, and J. J. L. Morton, Phys. Rev. A **82**, 022330 (2010).

[18] M. Schaffry, E. M. Gauger, J. J. L. Morton, J. Fitzsimons, S. C. Benjamin, and B. W. Lovett, Phys. Rev. A **82**, 042114 (2010).

[19] M. Müller, I. Lesanovsky, H. Weimer, H. P. Büchler, and P. Zoller, Phys. Rev. Lett. **102**, 170502 (2009).

[20] C. W. Mansell and S. Bergamini, New J. Phys. **16**, 053045 (2014).

[21] S. Boixo and R. D. Somma, Phys. Rev. A **77**, 052320 (2008).

[22] K. Modi, H. Cable, M. Williamson, and V. Vedral, Phys. Rev. X **1**, 021022 (2011).

[23] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).

[24] L. Chen, E. Chitambar, K. Modi, and G. Vacanti, Phys. Rev. A **83**, 020101 (2011).

[25] K. Modi, T. Paterek, W. Son, V. Vedral, and M. Williamson, Phys. Rev. Lett. **104**, 080501 (2010).

[26] D. Girolami, A. M. Souza, V. Giovannetti, T. Tufarelli, J. G. Filgueiras, R. S. Sarthour, D. O. Soares-Pinto, I. S. Oliveira, and G. Adesso, Phys. Rev. Lett. **112**, 210401 (2014).

[27] S. Kullback, *Information Theory and Statistics* (Dover, 1997).

[28] H. Cramér, *Mathematical Methods of Statistics* (Princeton University, Princeton, 1946).

[29] C. R. Rao, *Linear Statistical Inference and its Applications* (Wiley, New York, 1973).

[30] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

[31] If the control qubit is assumed to have initial state given by Eq. (5) then F_{q} is $\epsilon^2 l$, i.e. just as in DQC1 there is an overhead scaling with ϵ^2.

[32] K. Micadei, D. A. Rowlands, F. A. Pollock, L. C. Céleri, R. M. Serra, and K. Modi, New J. Phys. **17**, 023057 (2015).

[33] G. Y. Xiang, B. L. Higgins, D. W. Berry, H. M. Wiseman, and G. J. Pryde, Nature Photon. **5**, 43 (2011).

[34] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **96**, 010401 (2006).

[35] B. Dakić, V. Vedral, and Časlav Brukner, Phys. Rev. Lett. **105**, 190502 (2010).

[36] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).

Appendix A: State evolution throughout the protocol

We begin with the initial state

$$\sigma_0 = \frac{1}{2}\begin{pmatrix} |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}_2^{\otimes l} & |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}_2^{\otimes l} \\ |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}_2^{\otimes l} & |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}_2^{\otimes l} \end{pmatrix}. \tag{A1}$$

After the first CNOT we have

$$\sigma_1 = \frac{1}{2^{l+1}}\begin{pmatrix} |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}^{\otimes l} & |0\rangle\langle 1|^{\otimes n} \otimes (\rho_\epsilon\sigma_x)^{\otimes m} \otimes \sigma_x^{\otimes l} \\ |1\rangle\langle 0|^{\otimes n} \otimes (\sigma_x\rho_\epsilon)^{\otimes m} \otimes \sigma_x^{\otimes l} & |1\rangle\langle 1|^{\otimes n} \otimes (\sigma_x\rho_\epsilon\sigma_x)^{\otimes m} \otimes \mathbb{1}^{\otimes l} \end{pmatrix}. \tag{A2}$$

Next the phase is encoded, but note that u_ϕ commutes with $|0\rangle\langle 0|$, ρ_ϵ, and $\sigma_x\rho_\epsilon\sigma_x$

$$\sigma_2 = \frac{1}{2^{l+1}}\begin{pmatrix} |0\rangle\langle 0|^{\otimes n} \otimes \rho_\epsilon^{\otimes m} \otimes \mathbb{1}^{\otimes l} & e^{-i(n+1)\phi}\,|0\rangle\langle 1|^{\otimes n} \otimes (u_\phi\rho_\epsilon\sigma_x u_\phi^\dagger)^{\otimes m} \otimes (u_\phi\sigma_x u_\phi^\dagger)^{\otimes l} \\ e^{i(n+1)\phi}\,|1\rangle\langle 0|^{\otimes n} \otimes (u_\phi\sigma_x\rho_\epsilon u_\phi^\dagger)^{\otimes m} \otimes (u_\phi\sigma_x u_\phi^\dagger)^{\otimes l} & |1\rangle\langle 1|^{\otimes n} \otimes (\sigma_x\rho_\epsilon\sigma_x)^{\otimes m} \otimes \mathbb{1}^{\otimes l} \end{pmatrix}.$$

Next we apply the second CNOT gate

$$\sigma_3 = \frac{1}{2^{l+1}}\begin{pmatrix} \rho_\epsilon^{\otimes m} \otimes \mathbb{1}^{\otimes l} & e^{-i(n+1)\phi}(u_\phi\rho_\epsilon\sigma_x u_\phi^\dagger\sigma_x)^{\otimes m} \otimes (u_\phi\sigma_x u_\phi^\dagger\sigma_x)^{\otimes l} \\ e^{i(n+1)\phi}(\sigma_x u_\phi\sigma_x\rho_\epsilon u_\phi^\dagger)^{\otimes m} \otimes (\sigma_x u_\phi\sigma_x u_\phi^\dagger)^{\otimes l} & \rho_\epsilon^{\otimes m} \otimes \mathbb{1}^{\otimes l} \end{pmatrix} \otimes |0\rangle\langle 0|^{\otimes n}.$$

Finally we apply controlled-$v_{\theta(r)}$ as well as $v_{\theta(r)}$ on the control qubit. Note that $v_{\theta(r)}$ also commutes with $|0\rangle\langle 0|$, ρ_ϵ, and $\sigma_x\rho_\epsilon\sigma_x$. Measuring the control qubit in the basis of σ_x gives us

$$\begin{aligned} q^\pm(r) = \langle\pm|\sigma_4|\pm\rangle =& \frac{1}{2}\left(1 \pm \mathrm{Re}\{\mathrm{tr}[e^{-i(n+1)(\phi-\theta(r))}\,|0\rangle\langle 0|^{\otimes n} \otimes (\rho_\epsilon u_\phi\sigma_x u_\phi^\dagger\sigma_x v_{\theta(r)}^\dagger)^{\otimes m} \otimes (u_\phi\sigma_x u_\phi^\dagger\sigma_x v_{\theta(r)}^\dagger)^{\otimes l}/2^l]\}\right) && \text{(A3)} \\ =& \frac{1}{2}\left(1 \pm \mathrm{Re}\{e^{-i(n+1)(\phi-\theta(r))}\mathrm{tr}[\rho_\epsilon u_\phi\sigma_x u_\phi^\dagger\sigma_x v_{\theta(r)}^\dagger]^m\mathrm{tr}[u_\phi\sigma_x u_\phi^\dagger\sigma_x v_{\theta(r)}^\dagger]^l/2^l\}\right) && \text{(A4)} \\ =& \frac{1}{2}\left(1 \pm \mathrm{Re}\left\{e^{i(n+1)\omega(r)}\left[\cos(\omega(r)) + i\epsilon\sin(\omega(r))\right]^m\cos^l(\omega(r))\right\}\right). && \text{(A5)} \end{aligned}$$